What is Longer, Stronger, and Difficult to Guess?

Answer: Hopefully, YOUR password (or better yet, your passphrase)!

Here we are in 2024 and passwords are still ubiquitously used to protect our information from unauthorized access. Ideally, passwords that consist of a minimum of 15 to 20 random letters are fairly secure. Just don't base your password on anything that's easy for someone to learn about you, regardless of how long it is.

Did you know *it can take less than 10 minutes to crack a randomly generated 5-character password (like a password manager would create) that contains upper and lowercase letters, numbers, and symbols? Add one more character and it takes 12 hours to crack a 6-character password. But when you increase that by 5, to 11 characters, the time to crack increases to 2 million years. Even if you omit the symbols, an* ***11-character password with only upper and lowercase letters and numbers still takes 618 thousand years to crack****. Is your data worth the extra few characters and complexity?*

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090 | Password hash: bcrypt

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

› Learn more about this at hivesystems.com/password

According to Hive Systems, these statistics assume that an attacker is cracking your password from scratch. However, if your password has been previously stolen, uses simple (dictionary) words in a predictable way, or is reused across multiple sites and services, all bets are off. In this day and age, an attacker with a cache of stolen credentials has the ability/resources to crack your password in an instant – regardless of length or complexity.

Password managers for the win! There is no doubt that without a password manager, complex passwords are difficult to remember and lead us to the perpetual password pitfalls. As it is believed that the only secure password is one you can't remember, password managers are a great solution to help reduce some of the most common password fails – simple password creation, password reuse, password predictability, and passwords on "Post-It" notes. While some users may be reticent to use a password manager, it is widely heralded that the benefits far outweigh the risks. When it comes to password managers, consider this poignant statement (and associated timeless blog post) – "***Password managers don't have to be perfect, they just have to be better than not having one***," by Troy Hunt.

Peripheral points on producing potent passwords:

- **Create passphrases that are more easily remembered and more difficult to crack.** Passphrases of random words offer a fun alternative for creating longer stronger protection for your accounts. However, avoid using strings of common words or well-known phrases. (*Hint: Password managers create passwords too!*)
- **Longer is stronger.** Shorter passwords/passphrases are easily guessed or cracked. If a website or service does not allow passwords beyond 20 characters or so, mix upper and lowercase letters, numbers, and symbols in a **non-predictable way** to reduce the risk of them being cracked.
- **DON'T reuse passwords/passphrases.** When passwords are reused across multiple sites and services such as social media, banking, work-related, etc., only one set of leaked credentials can grant access to all of your accounts that use that same password/set of credentials.
- **DON'T use common words and expected substitutions.** Any word on its own is bad. Any combination of a few words, especially if they grammatically go together isn't great either.